

September 5, 2007

Office of the Secretary
Federal Trade Commission
Room H-135 (Annex K)
600 Pennsylvania Ave., NW
Washington, DC 20580

Submitted electronically: <https://secure.commentworks.com/ftc-SSNPrivateSector>

RE: SSNs In The Private Sector - Comment, Project No. P075414

To the Secretary and the Commission:

The Privacy Rights Clearinghouse (PRC) appreciates this opportunity to respond to the Federal Trade Commission's (FTC or Commission) request for comments on private sector use of the Social Security number (SSN). (1)

We are limiting our comments today to those situations where the SSN is collected from the consumer *solely* as a means of authenticating the identity of a consumer other than an SSN collection involving the extension of credit. We are also focusing on those situations where collection of the SSN is not required under Federal law. (2)

Our comments will therefore address two of the FTC's Topics for Comment:

2. The Role of the SSN as an Authenticator
5. The Role of the SSN in Identity Theft

Consumers often are coerced into providing an SSN as a means of authentication or verification, where appropriate authentication could be achieved through other means. A good example of this is when consumers attempt to opt out of prescreened credit card solicitations by calling 1-888-5-OPTOUT. (3) Another similar example is when consumers seek to obtain copies of their free annual credit reports either by calling 1-877-322-8228 or online at www.annualcreditreport.com.

Our PRC consumer hotline receives numerous calls from concerned individuals who are reluctant to provide this information either by telephone or online. They have heard the warnings about guarding their SSNs to protect themselves from identity theft. Yet paradoxically, they are afraid to take advantage of two important services that can help reduce their potential exposure to identity theft.

Because more than one person may share the same name or other identifying information, many believe that accurate identification of an individual generally works best when each individual has been assigned a unique identifying number. Many businesses, educational institutions, government agencies, and other organizations continue to believe that the SSN is the appropriate mechanism for achieving this purpose.

However, with the rise in the crime of identity theft and other fraudulent uses of the SSN, the continued use of the SSN as an identifier unnecessarily exposes consumers to fraudulent activity. PRC's list of recent security breaches demonstrates that databases containing lawfully collected SSNs are often inadequately protected against accidental or intentional disclosure. www.privacyrights.org/ar/ChronDataBreaches.htm

Moreover, transmission of SSNs online may subject consumers with inadequately protected computers to keyloggers, trojans, rogue websites, and other perils.

The challenge is to find a method of authentication that will uniquely identify an individual while protecting unnecessary disclosure and/or transmission of a consumer's SSN. We believe that the credit reporting agencies (CRA) are in a unique position to identify consumers without the need to resort to use of a consumer's full SSN.

We propose that the CRAs work to develop a methodology for uniquely identifying a consumer without requiring a consumer to disclose a full SSN when attempting to opt out of prescreened credit offers or when ordering a credit report. For example, the following combination of data would appear to be sufficient to uniquely authenticate and identify a specific consumer:

- Name
- Current address
- Previous address
- Date of birth
- Truncated SSN (for example, last 4 digits)

We recognize that any combination of data elements that serves the purpose of "replacing" the SSN as a unique authenticator or identifier has the potential itself to become a vehicle for identity theft and other fraudulent activity. The key to avoiding this problem is to continue to require a full SSN in those situations involving an extension of credit, while utilizing a truncated SSN in those situations solely requiring authentication or identification of an individual.

The concept of utilizing truncated SSNs in conjunction with other identifying information would seem to provide a workable alternative to the full SSN for the purpose of opting out of prescreened credit offers or ordering a credit report. However, this concept could also be extended to numerous other situations where the sole purpose of the SSN is either the creation a unique identifier or authentication of an individual's identity.

Again, the key to reducing exposure to identity theft and fraud would be to require full SSNs only in those situations where the purpose of the SSN collection is an extension of credit or is required by law.

We recommend that a study be conducted in order to test our suggestion regarding the use of multiple data elements as an alternative to full SSNs.

Thank you for your consideration of our comments.

Sincerely,

Beth Givens, Director
Paul Stephens, Director of Policy and Advocacy

Privacy Rights Clearinghouse
3100 5 th Ave., Suite B
San Diego, CA 92103
www.privacyrights.org

NOTES:

1. The Privacy Rights Clearinghouse (PRC) is a nonprofit consumer education and advocacy organization based in San Diego, CA, and established in 1992. The PRC advises consumers on a variety of informational privacy issues, including financial privacy, medical privacy and identity theft, through a series of fact sheets as well as individual counseling available via telephone and email. It represents consumers' interests in legislative and regulatory proceedings on the state and federal levels.

www.privacyrights.org

2. The Internal Revenue Service began using SSNs as taxpayer ID numbers in 1961. Therefore, SSNs are required on transactions in which the IRS may be interested. This includes most banking, investments, and real estate purchases, as well as employment records. Financial institutions are also required by federal law to participate in Customer Identification Programs that typically utilize SSNs.

3. Consumers who attempt to opt out online at www.optoutprescreen.com are requested, but not required to provide their SSN.